



Munich Personal RePEc Archive

# **Modern Risk Management Strategies for the Romanian State Treasury**

Cosma, Dorin and Cosma, Octavian

Faculty of Economics and Business Administration, West University,  
Timisoara, Romania

10 November 2009

Online at <https://mpra.ub.uni-muenchen.de/20425/>

MPRA Paper No. 20425, posted 04 Feb 2010 13:57 UTC

## Modern Risk Management Strategies for the Romanian State Treasury

*Disclosure and presentation of information are powerful tools for management monitoring and influencing entity behavior.*

Professor Dorin COSMA, PhD  
Faculty of Economics and Business Administration  
16 J.H.Pestalozzi Street, 300115, Timisoara, Timis, Romania  
dorin@cosma.ro

Ec. Octavian COSMA, PhD candidate  
Faculty of Economics and Business Administration  
16 J.H.Pestalozzi Street, 300115, Timisoara, Timis, Romania  
octavian@cosma.ro

### Abstract

This paper is exploring the introduction and modernization of corporative governance in public institutions, specifically in the Romanian State Treasury, by standardizing the risk evaluation in audit (RBIA). The authors are considering that achieving results in the country's progress is impossible by only implementing imported external solutions - for optimal results adjustments to internal and external historical characteristics and local interests are required. This requirement is reinforced by analyzing the economical developments that have taken place during the last 20 years (since migrating the economy from a centralized state to free markets), which also supports the authors' premise that further significant development is possible if the proper methods are put in place.

### Definition

- For **Management** [\[1\]](#) it is important to detect *risks*, to classify and deal with them in order of probability of occurrence and the imminence of the negative effect that they can produce, although not all risks can be addressed.

Internal audit helps the organization to achieve its *objectives* by assessing, through a systematic and methodical approach to its **risk management** processes, control and management of the company, making proposals to improve the effectiveness.

- **Risk Management** - involves a rational approach to risk identification, measurement, analysis and highlighting the most effective variants in terms of cost / benefit. Risk management process covers the following key stages:
  1. identification of risk;
  2. quantification and risk assessment;
  3. analysis, decision and planning quantities (plan and budget);
  4. operational risk management;
  5. risk monitoring;

6. *Reporting risk.*

- **Risk management** [2] - can be defined to be a systematic process involving human and material resources and based on risk analysis to achieve an optimal outcome.
- **Risk management** - methodology aimed at providing a comprehensive risk control, which helps maintain an acceptable level of exposure to public entity, with minimum costs. Risk management covers a wide range of activities strictly defined and organized, starting their conditions of existence and the fundamental objectives of the public entity and the risk factor in the design of an optimal and efficient operation.

Closely related to *risk management* is the concept of *management audit*.

The following is some *definition of management audit*:

1. **Audit management** [3] is an attempt to assess the performance of its various processes and functions.
  2. **TG Tokhe** "audit management has been defined as a critical by comprehensive management of all aspects of the process".
  3. **William P. Leonard** a comprehensive and constructive examination of an organizational structure of a company, institution or branch of government, plans, objectives and their operations.
  4. **Leslie R. Howard** is a management audit investigation business from highest to lowest order to clarify whether management measures have achieved their purpose by facilitating relations with the outside world's effective and efficient organization and smooth inside.
  5. **Taylor and Perry** audit management is a method of assessing the effectiveness of management at all levels of the organization, including investigation of business by an independent professional body ..
- **Risk management** can be achieved by addressing two directions:
  - *functional management*: identification, analysis, measurement limitations, monitoring, etc..
  - *operational management*: managing daily operations within the policies and procedures defined limits.

**Steps to initiate a process of risk management.**

Risk approach, prescribed by rules made the subject of many discussions and interpretations. In the following section we present different objectives.

Risk **management** approach [4] should focus on establishing policies, procedures and methods for conducting and monitoring the long-term activity, taking into account: optimizing value by quantifying risk, an overview of risk estimate, a conceptual framework for its for the organization's management and risk prevention, an adequate job in the sense of clearly defined responsibilities to improve decision making, according to the processes and functions - thus lowering the cost of monitoring.

**Objectives of risk management:**

- Future risk management within the entity to risk vulnerability, in order to provide a satisfactory level of assurance in respect of the objectives;
- Identification and internal audit events, transactions, transactions that may affect the entity's business objectives and expected results, monitoring the identified risks within the risk appetite;
- The strategy and identify events which may affect the entity, activity and results;

- Risk management is generated throughout the body, at every level, structure and form of organization, operation, internal audits provide a general and comprehensive perspective on risk
- Providing satisfying insurance to management and middle management.
- Targeting all processes to achieve all goals in one or more separate but connected categories with common features.

### **Specific stages of risk management**

- Identifying risks that may affect the effectiveness and efficiency of operations, the rules and regulations, confidence in the financial and internal management and external, to protect property, prevent and detect fraud;
- Establishing acceptable levels of risk exposure:
- Evaluation of the likelihood that the risk to occur and the size of its impact;
- Monitoring and evaluation of risks and adequacy of internal controls to manage risks;
- Verification reporting budget execution, including the involved programs.

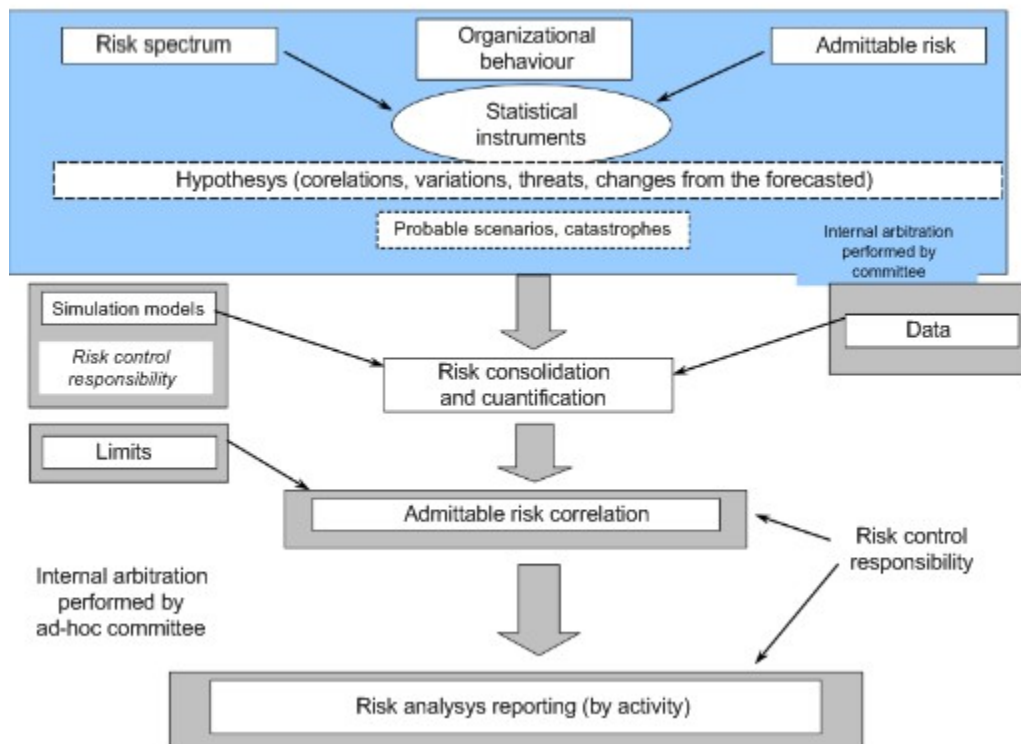
### **Features in the risk management process.**

Management Risk management is a complex process that begins by establishing an infrastructure and continuing the identification, analysis and risk assessment, measures to avoid or minimize losses, and financial decisions in the treatment necessary to minimize losses that cannot be avoided.

Given that studies have identified several *defining characteristics* of the risk management process:

- Risk management allows management decisions to facilitate communication between operators, regulators and public on the nature of the risks and their administration;
- Risk management requires appropriate and sufficient data to be developed, thus requiring a proper organization of information flows;
- Risk management is a process of management decision support;
- Risk management provides, structures and presents the best available risk information to support and facilitate the best management decisions;
- Risk management includes identification and risk analysis, identification, analysis and selection of alternative measures of risk control and performance evaluation;
- Risk management programs are structured, yet flexible, allowing them to be developed and adapted for different situations;
- Risk management is an integrative process;
- This risk can be ruled by cost-benefit analysis in the context of limited resources. Risk management logical structure, make consistent, documented, and clarifies the approach to choose, depending on uncertainties and benefits, the competitive alternatives;
- Risk management should cover the entire spectrum of risk, spreading from relatively common minor events, which pose small challenges, to those with very low likelihood but that may have very serious consequences;
- Risk management programs including performance measurement and call for monitoring, tracking and reporting processes in relation to expected results;
- Risk management involves gathering information from disparate areas and consolidating the results into a single "*picture*" which would give the complete snapshot of risk in the organization.

It can be said that risk management identifies and evaluates activities and occurrences that reduce the likelihood of events and consequences that may disturb the organization, leading to an increased safety level than before the application of risk management programs.

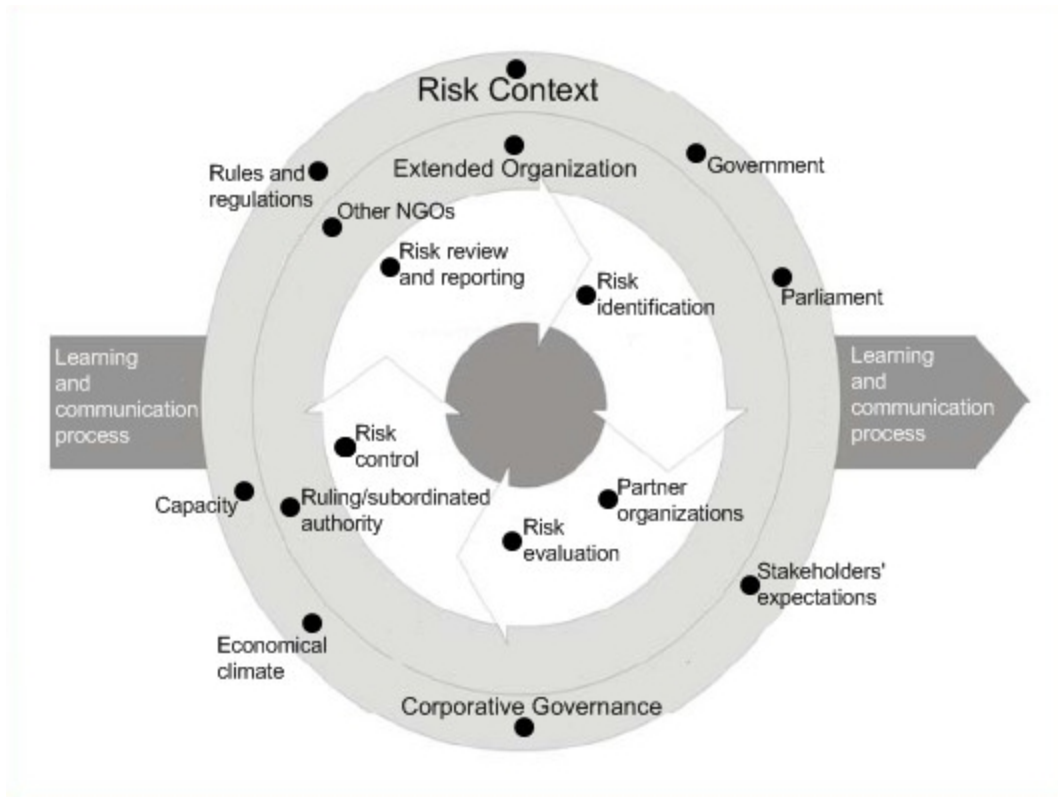


**Figure 1 - Managing risk for financial and accounting activities**

Source: adapted from Gerard Valdine, J.-F. Gavanou, C. Guttman, J. Le. Vourc'h, *Controller & Auditor*, Ed Dunod, 2006, p. 315.

## Risk management models

A risk management model provided by the Orange Book



**Figure 2 - The risk management provided by the Orange Book**

**Source: Orange book**

The analysis of the model reveals the following:

- The model must operate in an environment where the appetite for risk has previously been identified.
- Risk management is not a linear process, it is a way to balance a number of connected elements, which interact with each other and which must be in balance to each other if we are to effectively manage risks. Some specific risks can not be resolved independently of each other, and risk management may have an impact on another risk, or measures can be identified and implemented that will prove more effective in controlling multiple risks;
- The model divides the process of risk management in key components to illustrate them as suggestive, but in reality all these components are mixed in an ingenious way to create a single whole. A particular stage in which someone is on a certain risk need not necessarily be the same for all other risks.
- The model illustrates that the fundamental process of risk management is not isolated but takes place in a certain context and that some resources must be placed in the overall process to generate results that are intended to be achieved by managing risk.

### **B-The Risk Management developed the MFP**

The structured driven risk management process is shown in the figure below:



**Figure 3 - The Risk Management**

**Source:** Handbook on Methodology for implementation of standard internal control, risk management

The analysis of the model is based on the following characteristics:

- The idea that suggests that risk management does not relate to an isolated entity but an entity integrated in its existing environment, called context.
- This model divides the risk management process in components, arranged in a logical sequence of this process, but in reality, these components come together harmoniously to create a whole;
- Risk management is not a linear process, its components interacting all the time. Managing one risk can have an impact on other risks and steps identified as being effective measures to control risk may be beneficial in controlling other risks as well.
- Tolerability of risk (although not shown in picture above), is a key element in risk management process that characterizes every organization in part because defining the overall management practiced in that organization. A higher tolerance of risk is not necessarily bad, nor a lower tolerance does necessarily mean a good management. In conclusion, the tolerability of risk and resources related is the essential problem to find a balance between resources and benefits.
- Risk management is a continuous process of learning and implementing the necessary theoretical principles of risk management. What is particularly important in seeking to reach an effective risk management is continuously reinforcing an organizational culture of risk.

**C-Risk management model in the standard AS / NZS 4360/2001** [\[5\]](#)

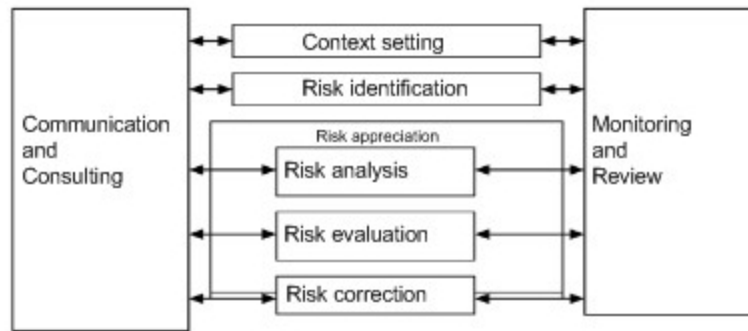


Figure 4 - Stages of the Risk Management Process

#### Remarks on model:

- **Establishing the context:** determining the strategic, organizational and risk management, and determine the structure analysis and the criteria against which risks will be assessed, identifying the affected parties / stakeholders and definition of communication and consultation;
- **Hazard identification:** identification as a basis for further analysis of what can happen, why and how, including hazards and associated consequences;
- **Risk analysis:** in terms of probability and severity, scope control and the effect of control measures on the severity of consequences, likelihood and severity of production can be combined to estimate the level of risk;
- **Evaluation and ranking of risk:** risk levels estimated by comparing pre-set criteria, continued risks can be ranked to identify priorities, risks identified as a low priority may be accepted without being treated, and become only subject to monitoring and review;
- **Treatment risks:** developing and implementing a management plan that should include considerations on the allocation of financial and other resources, and deadlines for action;
- **Communication and Consultation:** consultation and communication with affected parties / stakeholders, internal and external, every step of the process of risk management;
- **Monitoring and review,** monitor and review risk and performance assessment system of risk management and the changes it may affect.

#### D-A risk management model

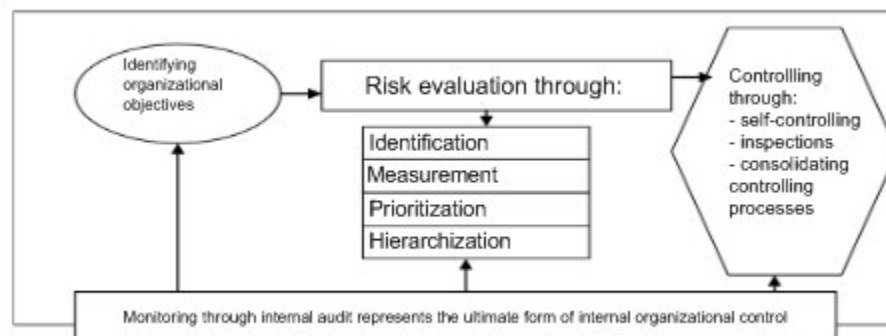


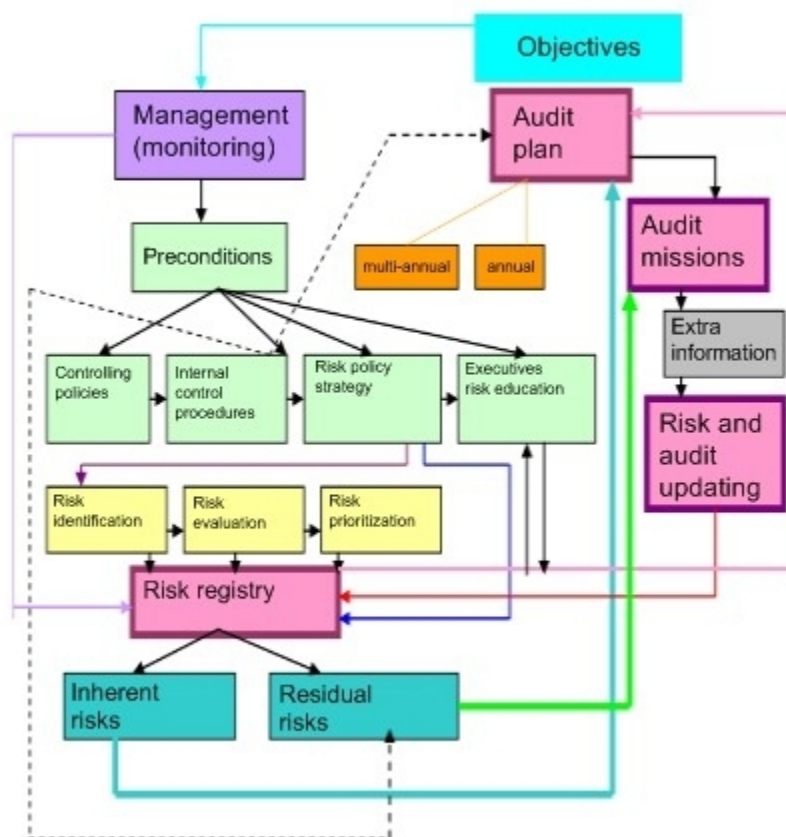
Figure 5 - Risk management model



Given the model, the risk management process involves the following steps:

- identify activities, operations;
- identify risks associated with them;
- determining factors / risk criteria;
- risk assessment;
- ranking / prioritization of risk;
- determining the person responsible for risk management;
- defining an action plan and monitoring compliance therewith;
- systematic reporting of the implementation of recommendations.

**E-Model the strategy of risk-based internal audit (RBIA), the State Treasury, created by author**



**Figure 6 - Circuit mechanism for implementing risk-based internal audit (RBIA)**

Source: made by author

As part of *corporate governance*, internal audit is undoubtedly circumscribed to the organizational culture, and plays an important role in the efforts made so that the entity is achieving its objectives. To achieve the strategies, managers are continuously engaged in finding solutions to meet changes in the economic environment. Therefore, it is natural that the internal audit position itself to

change over time. It is no longer a surprise that the State Treasury, in an attempt to achieve its goals, is constantly faced with new risks.

In a turbulent economic environment, the risks are diversified and sometimes influence, at times decisively, Treasury strategies.

The problem becomes acute, particularly in the event of an economic crisis. As shown in figure nr.58 at this stage in the State Treasury, for internal audit, *innovations* must be made to identify those activities with high risks in the treasury accounts following the switch from cash accounting to accrual accounting, which, as we have highlighted previously, is to be applied in the State Treasury. In my opinion, compared to the current system, the differences are firstly in order for the implementation of internal audit based on risk and secondly, to identify risks and their division into two categories: *inherent*, to be taken by audit plans (annual and triennial) and the *residual risks* that go directly to the jurisdiction of internal control and have a subsequent follow-up to date with the introduction of management. Once accrual accounting is introduced there are some new categories of risk, such as those arising from:

1. review accounting procedures and regulations, including the chart of accounts
2. appropriate training for staff
3. long period of time for implementation
4. computer system changes
5. getting the materiality
6. changing domestic and international legislation
7. change of auditable activities
8. absence of appropriate work procedures for audit
9. absence of procedures for controlling
10. lack of internal control and fully formalized
11. nonexistent history reporting system
12. fraud in economic factors
13. emergence of new categories of operation (foreign currency).

New categories of risk that are identified as being of interest to internal audit in the execution of phase shift in foreign currency in the State Treasury and especially the national implementation of the Single Euro Payments Area framework (*SEPA*) and migration to SEPA payment instruments, credit institutions, payment systems and payment service users in Romania, provided by the PSD (*Payments Services Directive*). At present, retail payments in national currency (which include payments to the State Treasury) had a large share in total non-cash payments, which makes automated clearing system the main channel for non-cash settlement payments in Romania.

These types of risks, which are added or existing ones listed in the passage of the new accrual accounting, are mainly these:

- a. Interest rate risk
- b. Risk of spread
- c. Foreign exchange rate (spot)
- d. Risk of dividend
- e. Risk index
- f. Volatility risk
- g. Counterparty risk
- h. Market risks which, in turn, may be  
H1-risk liquidity, solvency

H2-refinancing risk

H3-likelihood of recovery (time, money exchange, interest rate)

We believe that special attention must be given to the counterparty risk in these aspects:

- need for efficient back-office procedures to: pay, clearing, preservation of titles, confirmations
- expanding legal issues by establishing a contractual basis (existence, conditions), of law (European law or international), the netting site (bilateral, multilateral), notifications counterpart.

These risks can be assessed as inherent internal audit system and, consequently, will be subject to audit plans and procedures. Among the residual risks of internal control taken we are mentioning:

- a. insurance on the base material
- b. quality of internal audit
- c. failure to provide professional auditors
- d. drafting of internal regulations on controlling generalization
- e. risk of delivery of financial instruments
- f. setting margins in securities

Considering the multitude and diversity of risks, it requires, in our opinion, creating a nationwide *data bank* on all the risks faced by the Treasury, a resource that can be found and analyzed the internal auditors of State Treasury. This would avoid duplication, should speed up the objectives, would enhance the typology and would standardize procedures and working mechanisms.

**Taking into account the content of national and international professional standards in the Treasury, we believe that it should proceed to a reconsideration of how the application of the internal audit requirements by taking into account, in particular the rule of event risk on all its activities.**

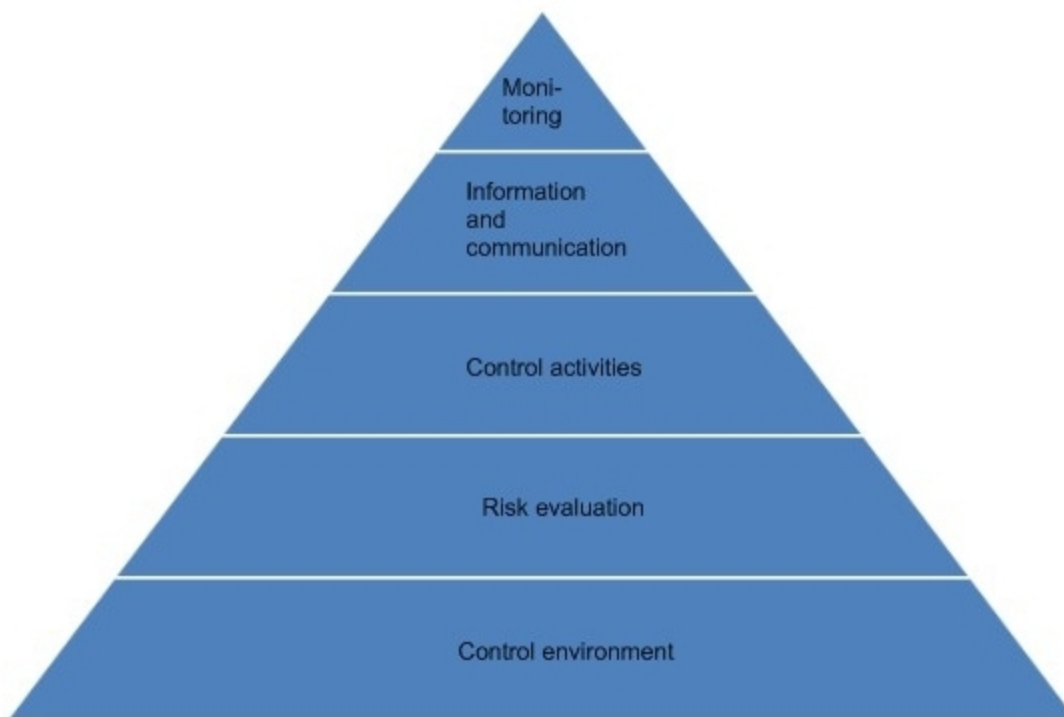
**To this end, we consider that, given the traditional methods used until now, it is necessary to achieve a methodology that better exploits the experience and opinions from internal audit practices based on risk.**

Such a change of strategy is based on dynamic adaptation of the Treasury financial and economic activity are having and profound change involving a first stage, a substantial effort, in terms of concept, but also organizational. It belongs in a broader context of concern to management on risks as *part of a good management practice*, and that *to be effective, risk management must become part of the culture of an organization*. To this *must be integrated into the philosophy, practices and business plans of the organization, rather than being viewed or practiced as a separate exercise*.

**Seen from this angle, we consider that the internal audit more effectively integrates the control system of the Treasury and makes a better connection with other control activities (in particular, internal control and controlling).**

Therefore, the control environment can be considered as a basis for good management / corporate governance.

The very model of management / corporate governance COSO (Committee of Sponsoring Organizations of the Treadway Commission), prescribe the five essential elements of it.



**Figure 7 - COSO Pyramid**

**Source:** Ana Morariu, Flavia Stoian, *Promoting corporate governance in the achievement of management, financial audit*, no.7/2006, Ed Chamber of Auditors of Romania, Standard, Australia / New Zealand, page 16

RBIA makes internal audit available to the Management Board, ensuring that their risk management processes are effectively managed in accordance with the entity's risk appetite. For the implementation RBIA in the Treasury, it is necessary to establish a methodology of work, including structures, methodologies and processes to be applied depending on their features. As shown in the literature, [6] certain preconditions must be met for implementing the strategy RBIA:

- knowledge of significant inherent risks (above the risk appetite);
- assess and prioritize risks;
- defining risk appetite and approval by management;
- set appropriate control policy internally;
- proper training of executives, in order to raise awareness, risk identification and monitoring control systems.

**We believe that this last prerequisite is crucial especially as regards the involvement of decision-makers, both in determining the risk/risk appetite, and especially, to create a team spirit in each organizational structure so that each employee can be trained in the knowledge of a number on high risks. Being successful in this endeavor depends if the entire community of employees is aware that controlling and internal audits offer guarantees of an efficient course of the organization. In this way, CEOs must create what in technical language means "Controlling animation. [7] This "phenomenon" is visible, especially in terms of updating risk categories included in the risk register.**

Preparing the Treasury to introduce RBIA can be achieved by the successive crossing of the following steps:

1. maturity assessment of risk, embodied in a register of risks, on which the auditors to formulate an opinion on the degree of control. With his help ensure the identification, knowledge of specific risk actions and effects on sectors of activity, and later to be managed and monitored. Once established, risks must be assessed in terms of reporting to a certain level of appetite for risk management, thereby creating an image of credibility and risk register.

In making it three procedures are used:

- interview;
  - seminars and to the identification of risks;
  - accounts;
  - of your sources.
- audit planning, aims to identify and periodization (annual or multiannual) areas, periods, structures that provide information management and security objectives, the management or monitoring of significant risks and is done by completing the audit plan, which contains elements:
    - determining risks included in the audit plan;
    - audits;
    - expected time;
    - name of the auditor;
    - approval of the Audit Committee;
    - the assurance to be in accordance with the internal audit charter;
    - consultancy activities, which will be given by the Treasury Management;
    - risks covered;

**Noted that depending on the complexity of objectives, audit plans are prepared by varying periods (less than a year, yearly, or longer). We appreciate that the Treasury aims are closely related to budgetary and fiscal policies and will be met by exercising appropriate control activities.**

**Given the conditions that Romania in its relationship with the European Union has, the rights and obligations multiannual budget (see Financial Perspective [\[8\]](#) EU 2007-2013), the exercise of internal audit, based on multi-annual audit plan, particular significance, in order to participate in the Treasury tax and budgetary policies to ensure consistency in Romania.**

3. achieving audit engagement as the basis of expression of the auditors, staff or the team. With this mission, there is an individuation of targets, in order to provide the Management Board, insurance, risk management and expression of opinion.

**In our opinion, this step is essential because, starting from a quasi-general consensus (a degree of ownership of risk according to the Register), to reach the formulation of objective picture of the Treasury in terms of prospects and risk exposures which are substance of recommendations that management will have to take into account. They have a corrective role in document management. For us, we appreciate that, given the current situation, those recommendations should obtain most often a mandatory status and therefore follow their achievement in perspective to be first met.**

4. update risk and therefore the scope of internal audit. For risk register to become credible, we believe that it should be updated whenever necessary. In this way,

by promoting the spirit of animation, which I mentioned above, to create even the motivation of employees (in general), auditors and managers (in particular), regarding the correctness of collective decision on risk management Treasury levels. In this way, we see the direct link, in itself, the risks and internal audit, hence the name RBIA as shown below:

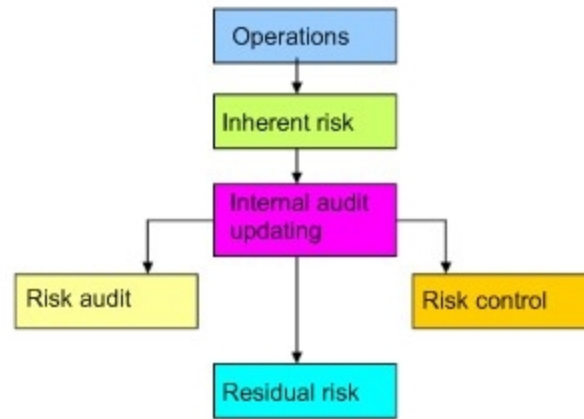


Figure 8 - Audit and risk.

Source: KH Spencer Pickett, *The Internal Auditing Handbook*, Ed Wiley, 1997, p. 229.

### **Analysis of components of risk management model.**

#### **Management strategies.**

*Achieving the perspective of risk management involves achieving the following activities:*

- Planning actions that must take place to achieve objectives;
- Plan actions necessary internal control and risk management integration into the general work plan (plan 1);
- Plan actions to be taken if risks materialize (plan 2).

Implementation Plan 1 and 2 are essential elements of a performance management that integrates in its structure and risk management. The measures taken in handling risk management are referred to the general theory of internal control internal control devices or instruments.

The diversity of devices / instruments of internal control is significant because all aspects of the organization's activities and the organization as a global entity, but can be classified into six main categories as follows:

- objectives;
- means;
- information system;
- organization, procedures;
- supervision.

#### **Description of steps to be achieved:**

##### **Step No. 1. Stability pounds strategy setting overall objectives.**

Each organization must develop their own policy-strategy of targeting the general. *"Goals are the positive effects that management tries to achieve or events / adverse effects that management tries to avoid"*.

**The general objectives** of any organization can be grouped into three categories, namely:

- Effectiveness and efficiency of operation;
- Reliability of internal and external information,
- Compliance with laws, regulations and internal policies.

*Standard [9] No.7 overall objectives of internal control must be consistent with the mission (objectives) of the public entity.*

### **Step No. 2. Setting specific goals and strategy determination thereof.**

After setting the general objectives to develop specific strategies for each component functions of the organization for setting goals and specific derivatives.

Specific and analytically developed, will take into account the following aspects:

- Management in terms of regularity, efficiency, economy and efficiency of general and specific risks of the public entity in furtherance of the commitments by developing its own strategy;
- Protection of public assets and public funds against losses due to error, waste, abuse or fraud.
- Respect and enforcement of all provisions (laws, regulations, decisions of management);
- Developing and monitoring information systems for collecting, storing, processing, updating and dissemination of data and information-communication and financial management and quality systems and procedures for the establishment of regular reporting.

Top managers and leaders and line managers, in addition to the general objectives will *define their mission and specific objectives*, taking into account the **characteristics such** as specified below:

- Be integrated to achieve the mission entrusted;
- Distribution of targets inside the function, in view of building a pyramid of objectives which all compete to achieve the general objective;
- The existence of opportunities to evaluate objectives expressed in real values, possible to achieve, quantitative or qualitative indicators of activity;
- Monitoring the achievement of objectives, through the management information system;
- Integration in time schedules;
- To be specific, clearly and avoiding confusion.

### **Step No.3. Policy development strategy decomposition-derived targets, specify:**

At this stage of managerial activities decompose goals derived specific functional components of the organization, the activities and analytical tasks related to each item of existing implementation of each compartment functional organizational structure. This work is done for the association and defining specific risk tasks, activities carried out within the organization, which may affect the objectives performance.

### **Risk analysis.**

In recent years, risk analysis is considered more common practice in all fields, serving in various possible options in choosing them. Have been developed for assessing macro-models, incorporating components for management options, there are complex interactions between these components and relationships "feedback". In these conditions every manager is encouraged to become its own risk manager.

**Risk analysis is a process** the risk "gross" results in the process of identifying risks are grouped, filtered and prioritized. The purpose of this activity is to provide detailed descriptions of risk

models for the organization so that the greatest risks and actions most appropriate risk control can be planned and implemented in the next step of the cycle of risk management.

- **Risk Analysis** is a risk assessment that can affect an organization. It starts with identifying threats, that is to gather as much data as possible, all foreseeable hazards. It is very important not to overlook any threats, which is why it is important to make use of comprehensive checklists. Once threats are known, the probability of manifestation and severity of their impact on the organization must be calculated. Since future events have a certain degree of uncertainty, estimating probability of materialization is done by a margin of error.
- **Risk analysis** is an active and dynamic process by which risks are systematically identified, analyzed and evaluated, so that it can provide a basis for future management decisions.

In the risk analysis process we are using the terms of inherent risk and residual risk.

**Inherent risk** is caused by exposure to a specific risk before any measures taken to mitigate it.

**Residual risk** is a certain risk due to exposure after mitigating measures being taken, and assuming that management's measures were effective. Risk mitigation measures are internal control. That residual risk is a measure of the effectiveness of internal control, for which some countries have replaced the term residual risk with the risk control.

**Risk Analysis** [\[10\]](#) is not an exact science. By establishing control activities to ensure that high risk to become average or low to any subsequent disappearance. However, risks have to "evolve" down.

#### **b. The steps of risk analysis.**

*Scheduled risk analysis management model established risk management played above:*

1. Identification of inherent risks;
2. Risk assessment and their quantification;
3. Risk prioritization:
  - Setting exposure;
  - Tolerance for risk assessment.
4. Application specific treatment residual risks, assessed, quantified and prioritized.

#### **1. Identifying risks involved.**

The risk in the work of a firm refers to the probability of missed objectives in terms of performance (lack of quality standards), program (deadline for implementation failure) and cost (budget overrun).

Risk factor is any factor that has a measurable probability to deviate from the plan. This of course assumes the existence of a plan. Strategies, plans and programs of the organization are elements that allow prefiguring reality and then confronting the actual outputs to expected results. To achieve the objectives should be running sets of activities. An activity denoted (a) may be seen as a risk if the following conditions are met:

$$0 < P(a) < 1 \quad (1)$$

$$P(a) = 1 = E(a) \quad (2)$$

$$L(a) = 0 \quad (3)$$

Where: **P(a)** = probability of an event (a) to occur;

**E(a)** = effect of the event (a) the objectives;

**L(a)** = monetary evaluation of **E(a)**.



During the identification phase of risk we are assessing potential dangers, effects and their likelihood to decide which of the risks must be prevented. Basically, at this stage we have to identify all elements that satisfy conditions (1), (2) and (3). Also, this eliminates the risks discrepancy, i.e. the elements of risk with low probability of occurrence or a negligible effect. This means those elements for which P (a) or L (a) tend to zero can be neglected. Hazard identification should be done regularly. It must consider both the risks as internal and external. Internal risks are risks that the management team can control or influence, while external risks are under control.

**Risk can be identified using various methods:**

- Preparation of checklists covering potential sources of risk, such as environmental conditions, expected results, staff, changes in objectives, errors and omissions in the design and implementation, cost estimates and lead times;
- Analysis of documents available in the company archives, to identify problems that occurred in situations similar to those of current;
- Using experience directly productive staff (heads of departments and teams) by inviting them to a formal meeting to identify risks. Often people on the ground are aware of the risks and problems that the office did not notify them. An effective land-office communication is one of the best sources of identification and mitigation;
- Identifying risks imposed from outside (through legislation, changes in economy, technology, relationships with unions) by appointing a person to attend meetings of professional associations, conferences and special publications to cover.

**2. Risk assessment and their quantification.**

There are three **principles** [\[11\]](#) of utmost importance to risk assessment:

- Ensure that there is a clearly structured process to consider both the likelihood as well as the impact of each risk;
- Recording of risk assessment in a way that facilitates monitoring and identifying the order of priorities of risks;
- To understand very clearly the difference between inherent risk and residual risk.

Evaluation should be based as far as possible on independent and unbiased evidence, to consider the full range of stakeholders affected by this risk and to avoid confusion between risk assessment and assessment of the acceptability of risk.

Risk assessment includes determining the probability of materialization of risks and impacts (consequences) on the objectives if they materialize. The combination of the estimated probability and estimated level of impact is exposure to risk in the risk profile that is achieved.

**Phases** required risk assessment activities:

- Evaluation of the likelihood of materializing the risk identified;
- Impact assessment objectives if the risk would materialize.

*Evaluation of the likelihood of materialization of risk*

**The probability of materialization of the risk**-opportunity or event that is a risk to materialize and is a measure for determining the possibility of developing risk quantification established favorable or when the nature of risk and available allow such an assessment. The probability is a measure of uncertainty is quantified by the percentage and the following reference levels: very low, low, medium, high, very high.

**Realizing the risk-** Translating from risk (possible) to the certainty (the fait accompli). The risk materialized becomes a possible problem in a difficult, if risk is a threat, or a favorable situation where risk is an opportunity.

***Impact assessment objectives if the risk materializes.***

The impact is the consequence to the objectives, which can be, depending on the nature of risk, positive or negative. The need for impact assessment is determined by the **organization's managers, and other personnel, are before a risk materializes, relative to individual objectives, and are measuring how big are the consequences of the objectives if the risk would materialize.** The impact of any risk is characterized by the consequences of different natures. Besides qualitative consequences, expressed descriptively, consequences in terms of budget (costs), effort (for work) and time (possible delay in time to achieve the objectives) can also be identified.

The impact of the risk may have the following components:

**Impact (I)**

- I<sub>C</sub> - Qualitative component (which may include quantitative indicators);
- I<sub>B</sub> - Budget component and / or heritage;
- I<sub>E</sub> - Component of effort;
- I<sub>T</sub> - Part time.

The impact is assessed against the following **reference levels: very low, low, medium, high, very high.**

### **3. Prioritizing risks.**

Once the risks are assessed, the organization will find out and assign priorities for the risks. The higher the risk exposure is, the more will that risk become a priority. Risks with the highest priority (major risk) must be constantly considered at the highest levels of the organization, and so must be the Council's attention constantly. Risk priorities will change over time as risks are addressed.

Specific activities to be undertaken:

- **Setting Exposure at risk.**

Exposure to risk is the sum of the consequences, **as a combination of probability and impact**, that an organization can be exposed to against predetermined objectives where the risk would materialize. Exposure to risk is a probabilistic concept, expressed as a combination of **probability** and **impact**. Thus, it has significance only in the production risk. After the occurrence risk is not an uncertainty, it becomes a fait accompli. In terms of probability theory this means that the likelihood (materialize) the risk is 1 (positive). Under these conditions exposure to risk is in fact impact. Grouping risks identified in an organization based on risk exposure lead to the risk profile the organization, which is documented and prioritized overall assessment of the range of specific risks facing the organization.

Inherent risk and residual risk are two aspects that the same risk: before the introduction of an instrument of internal control and after the introduction of an instrument of internal control. Therefore inherent risk exposure is a measure of "quantity" of risk they run organization that does not work the internal control system and exposure to residual risk is a measure of the amount of risk remaining after internal control was implemented. Because internal control is designed to mitigate the possibility of developing risk and / or mitigate the impact on objectives between the two exposures to risk, there is the relationship:

$$E_{\text{inherent risk}} > E_{\text{residual risk}}$$

Initial exposure to the inherent risk is determined by the "probability - high impact" before placing an instrument of internal control. After implementing the internal control, risk exposure will become the "low probability - low impact". A comparison of the two exposures that instrument of internal control is effective.

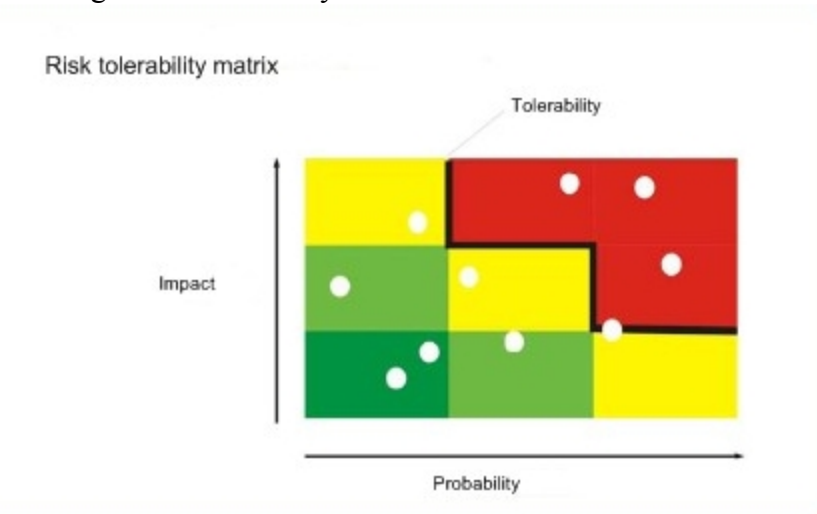
- **Tolerance for risk assessment.**

Risk tolerance is "quantity" of risk an organization is prepared to accept or is willing to expose itself at a time. The concept of risk tolerance have different meanings depending on the nature of risk, which may be an opportunity or a threat. When considering the opportunities, the concept of risk tolerance refers to an analysis of how much an organization is willing to risk while hoping to benefit from the related opportunities, and when considering threats, risk tolerance concerns tolerable exposure, justifiable to be achieved in practice.

Risk exposure (as a combination of probability and impact) as determined by an assessment makes sense only in relation to the level of risk tolerance. When exposure to risk compares to risk tolerance, the extent of risk control measures to be taken is obvious.

The absolute value of exposure to risk is less important than deviation exposure to risk tolerance. Simply put, the essential is if that risk is tolerable or not.

Below is the rendered figure on tolerability of risk:



**Figure 9 - Simple Tolerability Risk Matrix**  
**Source: Orange book**

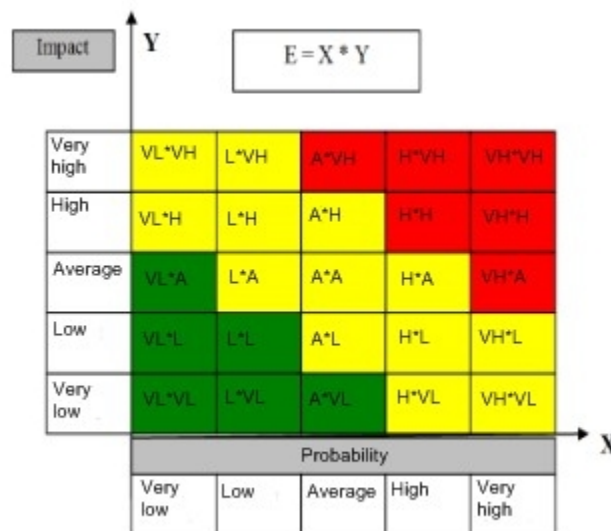
If exposure to inherent risk (risk ratio of internal control measures of risk) is less than or equal to the risk tolerance defined by managers then risk control measures are not required, which means that the risks are acceptable. Otherwise, control measures are needed so that risk of exposure to residual risk (risk remaining after risk control measures) to be within the risk tolerance limits set. Setting a limit of tolerance to risk is a problem to put in balance the "cost" (financial and/or other costs) exposure, where it would become reality. *The tolerance to risk is to find a balance between "cost" impacts and "cost" of risk control measures.* This means that all risks, which have a level

of exposure that are above the tolerance to be treated by measures that exposure to residual risks to be made under the threshold tolerance.

*Setting the tolerance to risk is a major act of managerial responsibility, because this is determined by risk exposure in conjunction with the cost of risk control measures.*

Intensity of control measures is directly proportional to the deviation of exposure to the tolerance established. Therefore, organizations applying risk management to general practice of using color in view the risk profile. For instance, the highest exposure risks which deviates most from the risk tolerance is used for red, which means that these risks cannot be accepted. Yellow (the attention limit) is used for risks whose exposure exceeds the limit of tolerance, but the deviation is moderate. The green color is represented, in general, by assumed risks, whose exposure is below the limit of tolerance.

The risk profile of organizations to implement practices described above have the following graphic:



**Figure 10 - Profile Risk Matrix - Risk map in an organization**

Risk profile, represented graphically above, resulting in pooling risks identified, evaluated and ranked in relation to the size bias from tolerance to risk exposure.

This creates an overview of the organization in terms of risk, but have a practical value of risk tables, which are structured to become operational risk management tools, presented in the form below:

Risk Name	Probability	Impact	Inherent risk Risk tolerance	Measures
Risk 1	H	VH	<b>H * VH</b>	Treatment by internal control risk
Risk 2	A	A	<b>A * A</b>	Tolerance to risk by maintaining internal control
Risk 3	VL	A	<b>VL * A</b>	No measures required

**Table 1 - Risk Table**

Note H, VH, AA, VL.A is the exposure and color intensity bias means exposure to risk tolerance. So, once the risk register is built, it must be brought to the attention of management for "refining" by identifying all *significant risks*, relative to *risk appetite*.

In the specialty literature sizing risk relevance (R) is classified in terms of both variable components of each risk: consequence (C), the probability (P). The relationship of calculation is:  $R = C * P$  model can be adapted or modified depending on the experience of auditors.

The connection between the two variables is expressed in the table below:

Sizing the relevance of risk		
If there is a risk, its consequences would be	OR, Likelihood risk is	Relevance of risk
1	2	3 = 1x2
Total or partial closure of the organization on a long time horizon (5)	Very high (5)	Very high (25)
Failure organization to achieve its objectives its major long time horizon (4)	High (4)	Big (16)
Failure organization to achieve certain goals on a limited time (3)	Average (3) (3)	Average (9)
The occurrence of damage without affecting the major goals of the organization (2)	Low (2)	Low (4)
The occurrence of minor damage, without affecting the objectives of the organization (1)	Very low (1)	Very low (1)

**Table 2 - Sizing relevance of risk**

Source: Financial Audit, nr.11/2008, pag.6.

On this basis, management defines its appetite for risk. One such model assessment of risks inherent meaning by reference to the appetite for risk may be:

The significance of the risks inherent appetite for risk in relation to the Board						
		Consequence of inherent risk				
		5	4	3	2	1
Likelihood of inherent risk	5	25	20	15	10	5

	4	20	16	12	8	4
	3	15	12	9	6	3
	2	10	8	6	4	2
	1	5	4	3	2	1

**Table 3 - Assessment of inherent risks**

Source: Financial Audit, nr.11/2008, pag.7.

In this way, the "head of internal audit will develop a risk-based audit plan to determine priorities for internal audit activities in accordance with the objectives of the organization" and "the internal audit program must be based on the risk assessment and be updated at least annually".

#### **4. Application specific treatment for residual, assessed, and quantified risks and their priorities**

The problem of controlling/not controlling risks is addressed in a relative manner, i.e. depending on tolerance. In this context we are speaking of risks that can not be controlled to a satisfactory level of exposure or risks only manageable in part.

##### ***Alternative strategies adopted to control risk [12].***

- **Accept-tolerated risk.** In this situation we do not take any measures, but should be ongoing monitoring risk to determine whether there is an increased level of exposure;
- **Transferring (outsourcing) Risk** is the risk of transmission to a destination outside the organization through an insurance policy or risk taking contract.
- **Treatment (mitigation) risk**-involves the application of appropriate control systems to reduce the inherent risk identified to a minimum or an appropriate level that can be tolerated.
- **Avoiding Risk** The risk response strategy is to eliminate activities (circumstances) that generate risks. It should be noted that the option of avoiding risk is significantly reduced in the public sector compared to the private sector.
- **Risk termination** is achieved by closure of the risk generating activity and can cause partial or failure in achieving the objective.
- **Handling difficult situations.**

Response to risk is the action phase of the cycle risk management which seeks: to eliminate risks, to reduce risks and/or to allocate risks.

Handling difficult situations means to develop plans aimed at reducing the impact if the risk materializes. **A strategy for difficult situations treatment is an alternative to other strategies,** but a supplementary one.

**Having determined the above issues, we conclude that treating risks is to keep them under control by measures of internal control.**

Tools/internal control devices can be addressed in depending of how they work in treating risk. We notice the following types:

- Tools/preventive internal control devices;
- Instruments/devices for internal control with remedial nature;
- Tools/for detective internal control;

- Tools /devices for directive internal control.

### C. Monitoring, review and reporting of risks.

- **Monitor risks.**

**Monitoring** is the activity in which risks are subject to an ongoing process of continuous surveillance to maintain their residual exposure under normal conditions, the tolerability accessible, acceptance of risk by quantification and its treatment.

The probability parameter is likely mainly supervised as the monitoring strategy applies to risk significant impact but low probability of occurrence.

- **Review and report risks.**

Review and reporting of risks is required for two reasons;

- Monitoring risk profiles change as a result of implementation of internal control instruments and changed circumstances favoring the emergence of risks;
- Getting assurance on the effectiveness of risk management and identifying the need to take further measures.

Review processes should be implemented to examine whether: risks persist, new risks have emerged, the impact and probability of risks have changed, internal control instruments are effectively put into work, some risks have climbed to upper management levels, etc. The results of the reviews should be reported to ensure continuous monitoring of the risk situation and to refer the major changes that require modification of priorities.

- **Features review activity:**

- Providing assurance that all aspects of risk management are reviewed at least once a year;
- Provide assurance that risks are subject to review at a frequency as established in relation to mobility of the circumstances and nature of internal control instruments to be implemented;
- Establish mechanisms for alerting of higher level management on emerging risks or risks already identified the changes so that these changes will be properly addressed.

### D. The purpose of the risk management process by completing the Registry of risks.

Good practice in the area recognized by the internal auditors have recommended that management develops *risk concerns* for each department, and by pooling their *risk register* will be achieved *the overall organizational risk*. The principle of corporate governance, transparency on virtually any control/inspections action and internal or external audits should start by looking at the *risks register* for the corresponding compartment. Development of the *Risk Register* will be completed in accordance with the model given by the UCASMFC register [\[13\]](#) of the MEF. The *Risk Register* includes residual and potential *risks*, but also the faced risks history (for the last 3-5 years) for each functional department and targets. A very important element is to establish responsibilities for coordinating the development of *the Registry* for updating systematic *risk* and its implication.

The *Risk Register* summary is shown below:





**Table 4 - Model summary of risk register.**

**Source: made by author**

where:

P-Probability; I-Impact; E-Exposure; RS-Responsible; MR-Monitored risk, IC-Internal control, R-Risk.

Where:

$$E = P * I$$

## Conclusion

Given the global economical developments that have taken place during the last years, better unified methods to assess and manage risks are needed in order to maintain economic growth. The authors believe that this document provides a new direction for auditing, based on risks and clearly in contrast with the old methods of testing or auditing, a methodology that can be implemented in virtually any related field. By using it, risks specific to different categories of operations are better covered. In our opinion, internal audits based on risk should lead to an optimal organization of all activities and can be achieved through ongoing assessment of internal control. Specifically, once risks in the activities of the State Treasury are identified, it is necessary to evaluate and classify them, and to base decisions on those findings, which will ensure maximum efficiency while minimizing exposure.

While our study extensively covers the Romanian State Treasury operations, the methods and procedures pertaining to risk management described therein can be implemented in any other public institution.

- 
- [1] M., Ghița, *Auditul intern*, Ed. Economică, București, 2004, pag. 115.
  - [2] Luminita Ristea- *Gestionarea riscurilor în cadrul administrațiilor finanțelor publice*, Revista finante publice si contabilitate nr 11-12/noiembrie-decembrie 2005, editata de M.E.F.. pag. 63.
  - [3] R.C.Bhatia, *Auditing*, Ed. VIKAS PUBLISHING HOUSE PVT LTD, New Delhi, 2004, pag 267.
  - [4] Ana Morariu, Anca Amuza Conabie, *Riscul managerial si auditul intern*, Revista audit financiar, nr.4/2007, editatade de C.A.F.R. pag 28.
  - [5] *Risk management*, Standards Australia/Standards Neew Zealand, Sydney/Wellington, 2001.
  - [6] D. Griffiths, *Risk based internal auditing : an introduction*, 2006, pag.26.
  - [7] M. Rouach, G.Naulleau, *Le controle de gestion bancaire et financier*, 3e, Banque editeur, 1998, pag.67.
  - [8] Elena-Doina Dascălu, *Sistemul bugetar în România*, Ed. Didactica și pedagogică, 2006, pag. 262.
  - [9] *Ordinul Ministrului Finanțelor Publice nr.946/2005* publicat în M.Of.nr.675/28.07.2005, pentru aprobarea codului controlului intern, cuprinzând standardele de management, control intern la entitățile publice și pentru dezvoltarea sistemelor de control managerial, Anexa nr.1.
  - [10] Marcel Ghiță, *Auditul Intern*, Ed. Economică, 2004, pag.120
  - [11] Cartea Portocalie-Gestionarea riscurilor- Principii și Concepte-Octombrie 2004 punctul 4.1. document publicat cu permisiunea Trezoreriei maiestății Sale din ANGLIA, *instituție echivalentă Ministerului de Finanțe din România*, în numele Imprimeriei Maiestății Sale, [www.hm-treasury.gov.uk](http://www.hm-treasury.gov.uk), tradus în România de M.F.P.



[12] A., Mitea, A., Băncuță, Ana Maria Polifrone, M., Ciucardel, *Auditul de sistem în instituțiile publice*, Ed. M.A.I. pag.95.

[13] Metodologia de implementare a standardelor de control, *Managementul riscurilor*, site MFP, pag. UCASMFC